(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
5. Juli 2001 (05.07.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/48974 A1

(51) Internationale Patentklassifikation[7]: H04L 9/30, G06F 7/72

(21) Internationales Aktenzeichen: PCT/EP00/13031

(22) Internationales Anmeldedatum:
20. Dezember 2000 (20.12.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 63 408.4 28. Dezember 1999 (28.12.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **DREXLER, Hermann** [DE/DE]; Oberländerstrasse 5a, 81371 München (DE). **VATER, Harald** [DE/DE]; An den Schulgärten 23, 35398 Giessen (DE).

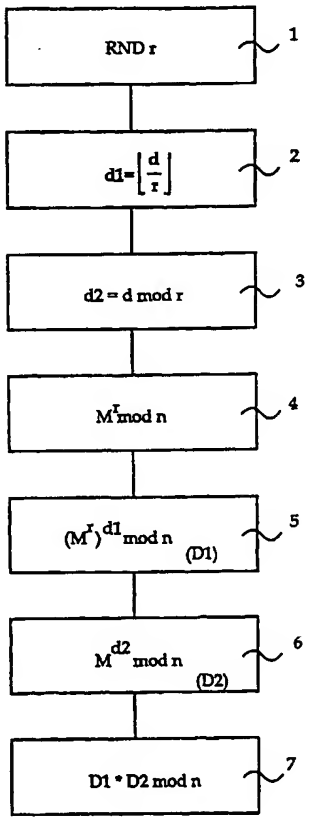
(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstr. 106, 80797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Fortsetzung auf der nächsten Seite]

(54) Title: PORTABLE DATA CARRIER PROVIDED WITH ACCESS PROTECTION BY DIVIDING UP CODES

(54) Bezeichnung: TRAGBARER DATENTRÄGER MIT ZUGRIFFSSCHUTZ DURCH SCHLÜSSELTEILUNG



(57) Abstract: The invention relates to a data carrier comprising a semiconductor chip provided with at least one memory in which an operating program is stored. Said operating program contains a number of instructions, whereby each instruction is elicited by signals that can be detected outside of the semiconductor chip. The aim of the invention is to protect secret data, which is provided in the chip of the data carrier, from "Differential Power Analysis" (DPA) or Higher Order DPA. To this end, the invention provides that in order to carry out security-relevant operations in the semiconductor chip, the data carrier is designed for dividing up secret data, which is stored or generated by the same, into at least three data parts, whereby an arithmetic unit for calculating a random number and for dividing the random number is contained therein, whereby the first data part is the integer result of the division, the second part is the remainder of the division, and the third part is the random number itself.

(57) Zusammenfassung: Die Erfindung betrifft einen Datenträger mit einem Halbleiterchip der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von ausserhalb des Halbleiterchips detektierbare Signale hervorruft. Es ist Aufgabe der Erfindung, geheime Daten, die im Chip des Datenträgers vorhanden sind, vor "Differential Power Analysis" (DPA) bzw. Higher Order DPA zu schützen. Gemäss der Erfindung ist der Datenträger ausgelegt, um zur Durchführung sicherheitsrelevanter Operationen im Halbleiterchip abgelegte oder von diesem generierte geheime Daten in mindestens drei Datenteile aufzuteilen, wobei eine Recheneinheit zum Berechnen einer Zufallszahl und zur Teilung der Zufallszahl enthalten ist, wobei der erste Datenteil das ganzzahlige Ergebnis der Teilung ist, der zweite Teil der Rest der Teilung und der dritte Teil die Zufallszahl selbst ist.

WO 01/48974 A1

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Tragbarer Datenträger mit Zugriffsschutz durch Schlüsselteilung

Die Erfindung betrifft einen Datenträger, der einen Halbleiterchip aufweist, in dem geheime Daten abgespeichert sind und verarbeitet werden.

Datenträger die einen Chip enthalten, werden in einer Vielzahl von unterschiedlichen Anwendungen eingesetzt, beispielsweise zum Durchführen von Finanztransaktionen, zum Bezahlen von Waren oder Dienstleistungen, oder als Identifikationsmittel zur Steuerung von Zugangs- oder Zutrittskontrollen. Bei allen diesen Anwendungen werden innerhalb des Chips des Datenträgers in der Regel geheime Daten verarbeitet, die vor dem Zugriff durch unberechtigte Dritte geschützt werden müssen. Dieser Schutz wird unter anderem dadurch gewährleistet, daß die inneren Strukturen des Chips sehr kleine Abmessungen aufweisen und daher ein Zugriff auf diese Strukturen mit dem Ziel, Daten, die in diesen Strukturen verarbeitet werden, auszuspähen, sehr schwierig ist. Um einen Zugriff weiter zu erschweren, kann der Chip in eine sehr fest haftende Masse eingebettet werden, bei deren gewaltsamer Entfernung das Halbleiterplättchen zerstört wird oder zumindest die darin gespeicherten geheimen Daten vernichtet werden. Ebenso ist es auch möglich, das Halbleiterplättchen bereits bei dessen Herstellung mit einer Schutzschicht zu versehen, die nicht ohne Zerstörung des Halbleiterplättchens entfernt werden kann.

Mit einer entsprechenden technischen Ausrüstung, die zwar extrem teuer aber dennoch prinzipiell verfügbar ist, könnte es einem Angreifer möglicherweise gelingen, die innere Struktur des Chips freizulegen und zu untersuchen. Das Freilegen könnte beispielsweise durch spezielle Ätzverfahren oder durch einen geeigneten Abschleifprozeß erfolgen. Die so freigelegten Strukturen des Chips, wie beispielsweise Leiterbahnen, könnten mit Mikro-

sonden kontaktiert oder mit anderen Verfahren untersucht werden, um die Signalverläufe in diesen Strukturen zu ermitteln. Anschließend könnte versucht werden, aus den detektierten Signalen geheime Daten des Datenträgers, wie z.B. geheime Schlüssel zu ermitteln, um diese für Manipulationszwecke einzusetzen. Ebenso könnte versucht werden, über die Mikrosonden die Signalverläufe in den freigelegten Strukturen gezielt zu beeinflussen.

In jüngerer Zeit sind überdies Methoden bekannt geworden, die es erlauben durch die Messung der Stromaufnahme oder des Zeitverhaltens bei der Verschlüsselung auf die geheimen Daten, insbesondere den geheimen Schlüssel zu schließen (Paul C. Kocher, „Timing attacks on implementation of Diffie-Hellman, RSA, DSS, and other Systems", Springer Verlag 1998; WO 99/35782).

Ein einfacher derartiger Angriff besteht in der „Simple Power Analysis" (SPA). Bei dieser Analysemethode wird beispielsweise eine bekannte Nachricht M einer Verschlüsselung mit einem geheimen Schlüssel d unterzogen, d.h. es wird der verschlüsselte Text $Y = M^d \bmod n$ gebildet. Bei der modularen Exponentiation wird bei einer "1" im Exponenten d eine Quadrier-Operation mit dem Zwischenergebnis und eine Multilizier-Operation mit M durchgeführt, während bei einer "0" in d nur eine Quadrier-Operation mit dem Zwischenergebnis ausgeführt wird. Bei bekanntem M kann durch die Beobachtung des Strom und/oder Zeitverhaltens während der Operationen die Nachricht M erkannt werden. Da diese immer bei Vorliegen einer "1" in d verwendet wird, kann ohne weiteres auf den Schlüssel geschlossen werden.

Diesem Angriff kann ohne weiteres durch einfache Änderungen in der Nachricht M bzw. im Schlüssel d begegnet werden. Aus Paul C. Kocher, „Timing Attacks on implementation of Diffie-Hellman, RSA, DSS, and other

Systems", Springer Verlag 1998 und der internationalen Patentanmeldung WO 99/35782 sind weitere Analysemethoden bekannt, bei denen auch bei geänderter, d.h. verschleierter Nachricht oder verschleiertem Schlüssel durch die Aufnahme einer Vielzahl von Meßkurven, in denen das Stromverhalten des integrierten Schaltkreises gemessen wird auf den Schlüssel geschlossen werden kann („Differential Power Analysis" (DPA) bzw. Higher Order DPA).

Als Sicherungsmaßnahme wurde ein sogenanntes „Exponent Blinding" vorgeschlagen, bei dem der geheime Schlüssel d nicht direkt verwendet wurde.

Zum einen kann anstelle des geheimen Schlüssels d für die Verschlüsselung $d+r^*\Phi$ verwendet werden, wobei r eine Zufallszahl und Φ die Eulersche PHI-Funktion ist. Speziell für den RSA-Algorithmus gilt: $n = p^*q$, wobei p und q Primzahlen sind und somit $\Phi = (p-1)^*(q-1)$ ist. Unter Anwendung des Eulers-Theorem gilt: $M^d \bmod n = M^{d+r^*\Phi} \bmod n$.
Wenn bei jeder Berechnung eine andere Zufallszahl r verwendet wird, kann auch bei einer Vielzahl von Analyse-Reihen nicht auf den Schlüssel d geschlossen werden.

Alternativ kann der geheime Schlüssel d in $d1^*d2 \bmod \Phi$ zerlegt werden. Es wird für die Verschlüsselung $Y=M^{d1^*d2 \bmod \Phi} \bmod n = (M^{d1})^{d2} \bmod n$.

Der Nachteil dieser Schutzmöglichkeit besteht jedoch darin, daß aus Mangel an Speicherplatz die Primzahlen p und q oder Φ üblicherweise nicht in einer Chipkarte abgelegt sind.

Der geheime Schlüssel d kann auch in eine Summe aus d1 und d2 zerlegt werden. Es gilt dann $d = d1 + d2$ bzw. für die Verschlüsselung:
$Y=M^{d1+d2} \bmod n = M^{d1} * M^{d2} \bmod n = (M^{d1} \bmod n * M^{d2} \bmod n) \bmod n$.

Um eine ausreichend hohe Sicherheit zu erhalten, muß bei der Zerlegung des Exponenten in d = d1 + d2 oder d = d1*d2 mod Φ für jede Berechnung ein neues, zufälliges d1/d2-Paar gewählt werden. Da die Erzeugung von Zufallszahlen in der Regel sehr langsam ist, eignet sich dieses Verfahren nicht zum Einsatz in Chipkarten. Zudem wird der Rechenaufwand für die modulare Exponentiation wesentlich erhöht, so daß auch dies gegen einen Einsatz in der Chipkarte spricht.

Es ist daher Aufgabe der Erfindung, geheime Daten, die im Chip eines tragbaren Datenträgers vorhanden sind, vor unberechtigtem Zugriff zu schützen, wobei der effiziente Einsatz der Daten nach wie vor gewährleistet sein soll.

Diese Aufgabe wird ausgehend vom Oberbegriff der Ansprüche 1 bzw. 7 und 12 durch die kennzeichnenden Merkmale des jeweiligen Anspruchs gelöst.

Die Erfindung gibt einen Datenträger mit einem Halbleiterchip der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von außerhalb des Halbleiterchips detektierbare Signale hervorruft, an.

Gemäß der Erfindung ist der Datenträger ausgelegt, um zur Durchführung sicherheitsrelevanter Operationen im Halbleiterchip abgelegte oder von diesem generierte geheime Daten in mindestens drei Datenteile aufzuteilen. Er enthält eine Rechner- bzw. Recheneinheit zum Berechnen einer Zufallszahl und zur Teilung der geheimen Daten durch die Zufallszahl. Der erste Datenteil besteht aus dem ganzzahligen Ergebnis der Teilung, der zweite Teil ist

durch den Rest der Teilung gegeben und der dritte Datenteil ist die Zufallszahl selbst.

Gemäß einer vorteilhaften Ausgestaltung der Erfindung bestehen die geheimen Daten aus dem geheimen Schlüssel für eine Verschlüsselung von Nachrichten, wobei vorzugsweise der geheime Schlüssel als Exponent bei der Berechnung von Gruppen-Operationen in asymmetrischen Verschlüsselungsverfahren (public-key-Verfahren, z.B. elliptische Kurven, RSA, usw.) bzw. von Modulo-Operationen eingesetzt wird.

Eine weitere Ausgestaltung der Erfindung sieht vor, daß die Zufallszahl so gewählt wird, daß die Länge der Zufallszahl zusammen mit dem Hamminggewicht der Zufallszahl bei verschiedenen Zufallszahlen etwa konstant ist. Auf diese Weise wird erreicht, daß aus der Zeitdauer, welche für die modulare Exponentiation, die proportional zur Länge des Exponenten und dem Hamminggewicht des Exponenten ist, nicht auf die geheimen Daten geschlossen werden kann.

Das erfindungsgemäße Verfahren sieht vor, daß der geheime Schlüssel durch eine vergleichsweise kurze Zufallszahl geteilt wird. Das Teilungsergebnis ohne Rest ergibt den ersten Teil des Schlüssels, der Rest ergibt den zweiten Teil des Schlüssels und die Zufallszahl den dritten Teil.

Für die Verschlüsselung einer Nachricht M gilt $Y = M^d \bmod n$. Der geheime Schlüssel d wird in d1, d2 und r aufgeteilt, wobei d1 = d/r (r ist eine Zufallszahl) ohne Rest gilt. Der Rest der Teilung ist der zweite Teil d2 des Schlüssels d. Damit gilt d2= d mod r. Für den Schlüssel d gilt somit d = r*d1 + d2.

Damit ergibt sich ein Verschlüsselungstext

$Y = M^d \bmod n = M^{r*d1 + d2} \bmod n = (M^r)^{d1} * M^{d2} \bmod n =$

$= ((M^r)^{d1} \bmod n * M^{d2} \bmod n) \bmod n.$

Der Ablauf der Bildung des verschlüsselten Textes Y ist in Fig. 1 dargestellt.

In Schritt 1 wird zunächst eine Zufallszahl r gebildet. Anschließend wird in Schritt 2 aus dem geheimen Schlüssel d durch Teilung mit der zuvor erhaltenen Zufallszahl r der erste Schlüsselteil d1 berechnet. Der zweite Teil d2 des Schlüssels wird durch Bildung von d mod r erhalten.

In Schritt 4 wird mit der Berechnung des Verschlüsselungstextes begonnen, indem zunächst $M^r \bmod n$ berechnet wird. Im nächsten Schritt 5 wird $D1 = (M^r)^{d1} \bmod n$ und in Schritt 6 wird $D2 = M^{d2} \bmod n$ berechnet.

Die Reihenfolge der einzelnen Rechenoperationen kann natürlich zum Teil auch zeitlich vertauscht werden. So kann zuerst $M^{d1} \bmod n$ berechnet werden und dann $(M^{d1})^r \bmod n$, da $(M^r)^{d1} \bmod n = (M^{d1})^r \bmod n$ ist.

Im letzten Schritt 7 werden die Zwischenergebnisse D1 und D2 miteinander multipliziert und der Modulo zu n gebildet. Es gilt damit

$D1 * D2 \bmod n = M^d \bmod n = Y.$

Die Erfindung hat den Vorteil, daß weder die Primzahlen p und q zur Bildung von Φ in der Karte gespeichert sein müssen und auch die Erzeugung langer Zufallszahlen, die sehr viel Rechenzeit in Anspruch nimmt, vermieden wird. Es wird weiterhin der Rechenaufwand für die Modulo-Operationen in Grenzen gehalten, so daß die erfindungsgemäße Lösung sowohl sicher als auch effizient in einer Chipkarte eingesetzt werden kann. Weiterhin müssen bei dem beschriebenen Verfahren keine Daten im nicht-

flüchtigen Speicher des Datenträgers abgeändert werden, was Zeit beanspruchen und zu einem Degradieren des nichtflüchtigen Speichers führen würde.

Da eine modulare Exponentiation eine Zeitdauer benötigt, die proportional zur Länge des Exponenten und des Hamminggewichts des Exponenten ist, kann eine zusätzliche Erhöhung der Sicherheit erreicht werden, wenn für die Erzeugung der Zufallszahl r ein Verfahren gewählt wird, bei der die Länge von r und das Hamminggewicht von r eine Konstante ergibt.

Die Erfindung kann für eine Vielzahl von Verschlüsselungssysteme angewendet werden. Es sei beispielhaft auf die RSA-Verschlüsselung, die Verschlüsselung nach ElGamal, DSA, Elliptische Kurvensysteme usw. verwiesen.

Patentansprüche

1. Datenträger mit einem Halbleiterchip der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von außerhalb des Halbleiterchips detektierbare Signale hervorruft, dadurch **gekennzeichnet**, daß der Datenträger ausgelegt ist, um zur Durchführung sicherheitsrelevanter Operationen im Halbleiterchip abgelegte oder von diesem generierte geheime Daten in mindestens drei Datenteile aufzuteilen, wobei eine Recheneinheit zum Berechnen einer Zufallszahl und zur Teilung der Zufallszahl enthalten ist, wobei der erste Datenteil das ganzzahlige Ergebnis der Teilung ist, der zweite Teil der Rest der Teilung und der dritte Teil die Zufallszahl selbst ist.

2. Datenträger nach Anspruch 1, dadurch **gekennzeichnet**, daß die geheimen Daten ein geheimer Schlüssel für eine Verschlüsselung von Nachrichten sind.

3. Datenträger nach Anspruch 1 oder 2, dadurch **gekennzeichnet**, daß die geheimen Daten als Exponent bei der Berechnung von Gruppen-Operationen in asymetrischen Verschlüsslelungsverfahren Verwendung finden.

4. Datenträger nach einem der Ansprüche 1 bis 3, dadurch **gekennzeichnet**, daß die geheimen Daten als Exponent bei der Berechnung von Modulo-Operationen eingesetzt werden.

5. Datenträger nach einem der Ansprüche 1 bis 3, dadurch **gekennzeichnet**, daß der geheime Schlüssel als Exponent bei der Berechnung von Modulo-Operationen eingesetzt wird.

6. Datenträger nach einem der Ansprüche 1 - 5, dadurch **gekennzeichnet**, daß die Zufallszahl so gewählt wird, daß die Länge der Zufallszahl zusammen mit dem Hamminggewicht der Zufallszahl bei verschiedenen Zufallszahlen etwa konstant ist.

7. Verfahren zur Sicherung geheimer Daten in Datenträgern mit einem Halbleiterchip der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von außerhalb des Halbleiterchips detektierbare Signale hervorruft, dadurch **gekennzeichnet**, daß zur Durchführung sicherheitsrelevanter Operationen im Halbleiterchip abgelegte oder von diesem generierte geheime Daten in mindestens drei Datenteile aufgeteilt werden, wobei zunächst eine Zufallszahl berechnet wird und der erste Datenteil aus dem ganzzahligen Ergebnis einer Teilung der geheimen Daten durch die Zufallszahl ist, der zweite Teil aus dem Rest der Teilung besteht und der dritte Teil die Zufallszahl selbst ist.

8. Verfahren nach Anspruch 7, dadurch **gekennzeichnet**, daß die geheimen Daten ein geheimer Schlüssel für eine Verschlüsselung von Nachrichten sind.

9. Verfahren nach Anspruch 7 oder 8, dadurch **gekennzeichnet**, daß die geheimen Daten als Exponent bei der Berechnung von Gruppen-Operationen in asymetrischen Verschlüsselungsverfahren Verwendung finden.

10. Verfahren nach Anspruch 7 oder 8, dadurch **gekennzeichnet**, daß die geheimen Daten als Exponent bei der Berechnung von Modulo-Operationen eingesetzt werden.

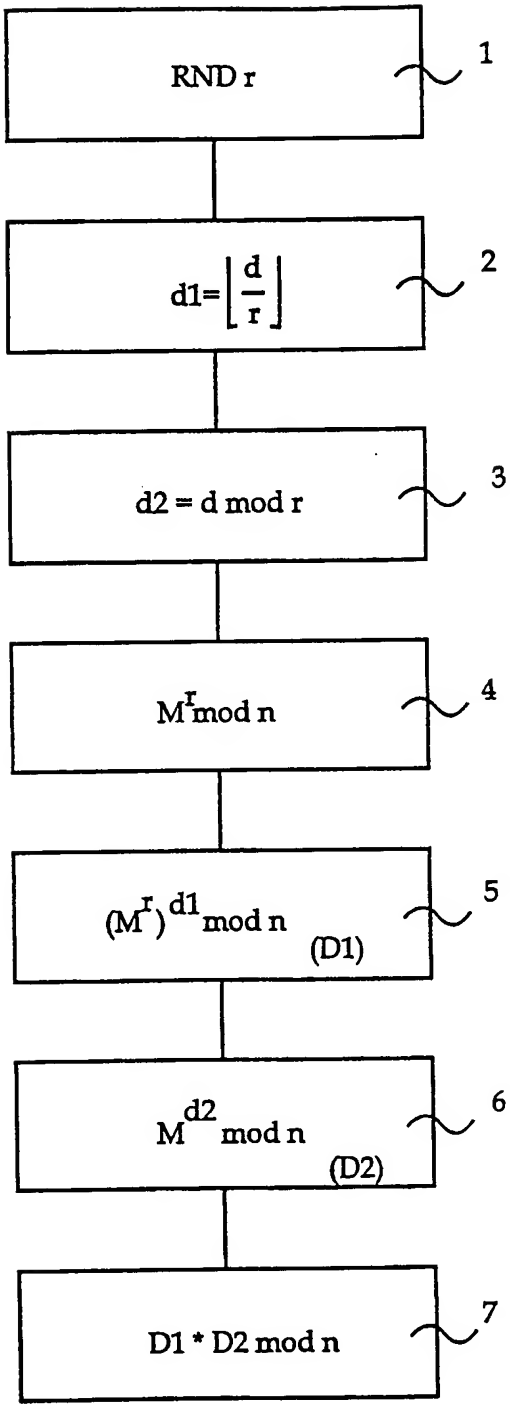
11. Verfahren nach Anspruch 7 oder 8, dadurch **gekennzeichnet**, daß der geheime Schlüssel als Exponent bei der Berechnung von Modulo-Operationen eingesetzt wird.

12. Verfahren nach einem der Ansprüche 7 - 11, dadurch **gekennzeichnet**, daß die Zufallszahl so gewählt wird, daß die Länge der Zufallszahl zusammen mit dem Hamminggewicht der Zufallszahl bei verschiedenen Zufallszahlen etwa konstant ist.

13. Verfahren zur Bildung einer verschlüsselten Nachricht in einem System zur Authentisierung von Systemkomponenten oder zur Bildung einer Signatur, dadurch **gekennzeichnet**, daß

- eine Zufallszahl r gebildet wird,
- aus einem geheimen Schlüssel d durch Teilung mit der zuvor erhaltenen Zufallszahl r ein erster Schlüsselteil (d1) berechnet wird,
- ein zweiter Teil (d2) des Schlüssels durch Bildung von d mod r erhalten wird,
- mit der Berechnung des Verschlüsselungstextes begonnen wird, indem M^r mod n berechnet wird,
- $D1 = (M^r)^{d1}$ mod n und $D2 = M^{d2}$ mod n berechnet wird und
- die Zwischenergebnisse D1 und D2 miteinander multipliziert und der Modulo zu n gebildet wird.

14. Verfahren nach Anspruch 13, dadurch **gekennzeichnet**, daß zur Berechnung von D1 zunächst M^{d1} mod n und nachfolgend $(M^{d1})^r$ mod n berechnet wird.


RND r
1
$d1=\left\lfloor \frac{d}{r} \right\rfloor$
2
d2 = d mod r
3
$M^r \bmod n$
4
$(M^r)^{d1} \bmod n$ (D1)
5
$M^{d2} \bmod n$ (D2)
6
D1 * D2 mod n
7

INTERNATIONAL SEARCH REPORT

Interna ıal Application No
PCT/EP 00/13031

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KOCHER P C: "TIMING ATTACKS ON IMPLEMENTATIONS OF DIFFIE-HELLMAN, RSA, DSS, AND OTHER SYSTEMS" 16TH. ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, AUG. 18 - 22, 1996. PROCEEDINGS,BERLIN, SPRINGER,DE, vol. CONF. 16, 18 August 1996 (1996-08-18), pages 104-113, XP000626590 ISBN: 3-540-61512-1 cited in the application page 111 -page 112 --- -/--	1-14

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" *earlier document but published on or after the international* filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 March 2001	06/04/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/EP 00/13031

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	MESSERGES T S ET AL: "Power analysis attacks of modular exponentiation in smartcards" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP,XX,XX, August 1999 (1999-08), pages 144-157, XP000952221 page 155 -page 156	1-14

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Interna. ales Aktenzeichen
PCT/EP 00/13031

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/30 G06F7/72

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, INSPEC, PAJ, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	KOCHER P C: "TIMING ATTACKS ON IMPLEMENTATIONS OF DIFFIE-HELLMAN, RSA, DSS, AND OTHER SYSTEMS" 16TH. ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, AUG. 18 - 22, 1996. PROCEEDINGS,BERLIN, SPRINGER,DE, Bd. CONF. 16, 18. August 1996 (1996-08-18), Seiten 104-113, XP000626590 ISBN: 3-540-61512-1 in der Anmeldung erwähnt Seite 111 -Seite 112 --- -/--	1-14

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[ ] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
28. März 2001	06/04/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

1

INTERNATIONALER RECHERCHENBERICHT

Interna ales Aktenzeichen
PCT/EP 00/13031

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	MESSERGES T S ET AL: "Power analysis attacks of modular exponentiation in smartcards" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP,XX,XX, August 1999 (1999-08), Seiten 144-157, XP000952221 Seite 155 -Seite 156	1-14

1